CLAIMS

What is claimed is:

1. A method of updating an electronic device, the method comprising:

receiving a notification in the electronic device; and

determining the authenticity of the notification in the electronic device.

2. The method according to claim 1, further comprising:

informing the electronic device of availability of at least one update package for updating at least one of firmware and software resident in the electronic device; and

simultaneously informing a notification history server that a notification has been sent to the electronic device.

3. The method according to claim 1, wherein determining the authenticity of the notification comprises contacting a notification history server, the notification history server keeping a record of notifications sent to the electronic device.

4. The method according to claim 1, further comprising:

ignoring the notification in the electronic device upon determining that the notification is inauthentic;

recording that an inauthentic notification has been received; and

waiting to receive another notification in the electronic device.

5. The method according to claim 1, further comprising determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is authentic.

6. The method according to claim 5, further comprising:

retrieving the update package; and

performing an update of at least one of firmware and software resident in the electronic device.

7. The method according to claim 1, wherein the notification comprises one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

8. The method according to claim 1, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

9. The method according to claim 1, wherein determining the authenticity of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server.

10. The method according to claim 9, wherein an authorized server comprises one of a management server and a customer care center.

11. The method according to claim 1, wherein the notification comprises location and identification information regarding a management server providing access to an update package and information regarding the update package.

12. The method according to claim 11, wherein location and identification information comprise at least one of a universal resource locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

13. The method according to claim 1, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event.

14. The method according to claim 13, wherein retrieving the update package from the default management server is performed after authentication of the notification message.

15. The method according to claim 1, further comprising:

retrieving an update package via a download agent in the electronic device; and

updating at least one of firmware and software in the electronic device via an update agent in the electronic device.

16. The method according to claim 1, further comprising preventing unauthorized updates of at least one of firmware and software in the electronic device.

17. The method according to claim 16, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic.

18. The method according to claim 16, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

19. The method according to claim 1, further comprising provisioning an address of a management server in the electronic device during a bootstrap provisioning event by sending a notification. the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

20. A mobile services network at least comprising:

at least one electronic device;

a management server communicatively linked with the at least one electronic device via a communication link; and

a notification history server operatively connected to the management server, the notification history server comprising a record of authentic notifications sent to the at least one electronic device.

21. The network according to claim 20, wherein the electronic device at least comprises:

non-volatile memory;

a short message entity;

random access memory; and

security services.

22. The network according to claim 21, wherein the non-volatile memory in the electronic device at least stores:

an update agent;

a firmware and real-time operating system;

an operating system layer;

a download agent or browser; and

an end-user related data and content.

23. The network according to claim 20, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

24. The network according to claim 20, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server, the electronic device being adapted to determine the authenticity of the notifications by contacting the notification history server.

25. The network according to claim 24, wherein the notification history server is adapted to determine whether a notification is authentic by examining message identification information in the notifications.

26. The network according to claim 24, wherein the electronic device is adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authentic.

27. The network according to claim 24, wherein the electronic device is adapted to determine whether a notification originated from an authorized sender.

28. The network according to claim 27, wherein an authorized sender is at least one of the management server and a customer care center resident in the network.

29. The network according to claim 20, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages.

30. The network according to claim 20, wherein notifications comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

31. The network according to claim 30, wherein notifications further comprise at least one user data field containing message identification information.

32. The network according to claim 30, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package.

33. The network according to claim 32, wherein location and identification information comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

34. The network according to claim 20, wherein upon determining that a notification received in the electronic device is inauthentic, the electronic device is adapted to ignore the notification and wait for another notification, and a record is created recording that an inauthentic notification has been received.

35. The network according to claim 20, wherein the management server comprises the notification history server and an update package repository.

36. The network according to claim 20, wherein the notification history server is incorporated into a short message center in the network.

37. The network according to claim 20, further comprising a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device.

38. The network according to claim 37, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic.

39. The network according to claim 37, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

40. The network according to claim 20, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification. the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.